Cryptanalysis of Goriparthi et al.'s Bilinear Pairing Based Remote User Authentication Scheme

Hae-Jung Kim, Eun-Jun Yoon

Cryptanalysis of Goriparthi et al.'s Bilinear Pairing based Remote User Authentication Scheme

Hae-Jung Kim[1] and Eun-Jun Yoon[2,*]

[1] College of Liberal Education, Keimyung University,
1000 Sindang-dong, Dalseo-Gu, Daegu 704-701, Republic of Korea
[2] Department of Cyber Security, Kyungil University,
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
hjkim325@hanmail.net, ejyoon@kiu.ac.kr

Abstract. Recently, many user authentication schemes with bilinear pairings have been proposed for client-server environment. In 2009, Goriparthi et al. proposed an improved bilinear pairing based remote user authentication scheme. Goriparthi et al. claimed that the improved scheme can withstand replay, forgery and insider attacks. However, this paper shows that the improved scheme is not only insecure against off-line password guessing, remote server impersonation, Denial of Service, and insider attacks, but also has mutual authentication problem.

Keywords: Cryptography, Authentication, Security, Attack, Smart card, Bilinear pairing.

1 Introduction

A remote user authentication scheme allows users to access various services offered by the remote server. In 1981, Lamport [1] first introduced well-known password authentication scheme with one-way hash function, but the scheme suffers from high hash computation overhead and password resetting problems. Thereafter, many authentication schemes have been proposed based on hash function and on public key cryptography [2–7]. The identity-based public-key system with bilinear pairings defined on elliptic curves offers a flexible approach to achieve simplifying the certificate management [8]. Bilinear pairings are an effective method to reduce the complexity of the discrete log problem in a finite field and provides a good setting for the bilinear Diffie-Hellman problem (BDHP). In the past, many user authentication schemes with bilinear pairings have been proposed for client-server environment [9–11].

In 2004, Das et al. [9] first proposed a remote user authentication scheme using bilinear pairings. However, Chou et al. [10] pointed out that Das et al.'s scheme is

* Corresponding author: Eun-Jun Yoon(ejyoon@kiu.ac.kr) Tel.: +82-53-850-7291; Fax: +82-53-850-7609

insecure to replay attack and the proposed a modified scheme to over- come replay attack. In 2009, Goriparthi et al. [11] showed that Chou et al.'s modified scheme still suffers from the replay attack and then proposed another improved GDS scheme to overcome replay, forgery and insider attacks.

Nevertheless, this paper shows that the GDS scheme is not only insecure against off-line password guessing, remote server impersonation, Denial of Service (DoS), and insider attacks, but also has secure mutual authentication problem. As a result, the GDS scheme cannot be applicable to real client-server communication environments.

This paper is organized as follows: Section 2 describes the basic definition and properties of the bilinear pairings. Section 3 reviews the GDS scheme; then Section 4 discusses its weaknesses. The conclusions are presented in Section 5.

2 Preliminaries

This section describes the basic definition and properties of the bilinear pairings[8–11].

2.1 Bilinear pairings

Let G_1 be an additive cyclic group of prime order q and G_2 be the multiplicative cyclic group of the same order. Practically we can think of G_1 as a group of points on an elliptical curve over Z_q^*, and G_2 as a subgroup of the multiplicative group of a finite field $Z_{q^k}^*$ for some $k \in Z_q^*$. Let P be a generator of G_1. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ having the following three properties:

1. Biliearity: $e(aP, bQ) = e(P, Q)^{ab}$, for all $P, Q \in G_1$ and $a, b \in Z_q^*$.
2. Non-degeneracy: For all P, where P is not a generator, there exists $Q \in G_1$. such that $e(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ in polynomial time for all $P, Q \in G_1$.

2.2 Computational problems

Many pairing-based cryptographic schemes are based on the hardness of the following problems. No algorithm is known to be able to solve any of them so far.

Definition 1. *Given a group G_1 of prime order q, a generator P of G_1, the computational Diffie-Hellman problem (CDHP) is to compute abP given (P, aP, bP) for $a, b \in Z_q^*$.*

Definition 2. *Given two groups* G_1 *and* G_2 *of the same prime order* q*, a bilinear map* $e: G_1 \times G_1 \to G_2$ *and a generator* P *of* G_1*, the bilinear Diffie-Hellman problem (BDHP) in* (G_1, G_2, e) *is to compute* $h = e(P,P)^{abc}$ *given* (P, aP, bP, cP) *for* $a, b, c \in Z_q^*$.

Definition 3. *Given a group* G_1 *of prime order* q*, a generator* P *of* G_1*, the elliptic curve factorization problem (ECFP) is to find* xP *and* yP *given* $xP + yP$ *for* $x, y \in Z_q^*$.

Definition 4. *Elliptic curve discrete logarithm problem (ECDLP): Given a group* G_1 *of prime order* q*, two elements* P *and Q, find an integer* $a \in Z_q^*$*, such that* $Q = aP$ *whenever such an integer exists.*

3 Review of GDS Scheme

GDS scheme [11] consists of three phases namely Registration; Login and Verification; and Password Change Phases and the phases work as follows. Throughout the paper, notations are employed in Table 1.

Table 1. Notations used in GDS scheme.

U, RS	The user and the remote server, respectively.
ID	The identity of U.
e	A bilinear map, $e: G_1 \times G_1 \to G_2$.
P	A generator of group G_1.
PW	Password of U.
N	A user friendly random number of U.
s	The private key of RS in Z_q^*.
P_S	The public key of RS such that $P_S = sP$.
sk	A common session key shared between U and RS.
$H(\cdot)$	A map-to-point function, $H: \{0,1\}^* \to G_1$.
$h(\cdot)$	One way hash function, $h: \{0,1\}^* \times G_1 \to \{0,1\}^k$, where k is output length.

3.1 Registration phase

This phase is depicted in Figure 1. When the user U wants to register to the remote server RS.

R1. $U \rightarrow RS: (ID, PW)$

U submits his/her identity ID and password PW to the RS.

R2. $RS \rightarrow U: (ID, R_{ID}, H(\cdot), h(\cdot))$

(a) RS computes U 's private key $R_{ID} = sH(ID) + H(PW)$ by using the private key s.

(b) RS personalizes the smart card with $(ID, R_{ID}, H(\cdot), h(\cdot))$ and hands it to U securely.

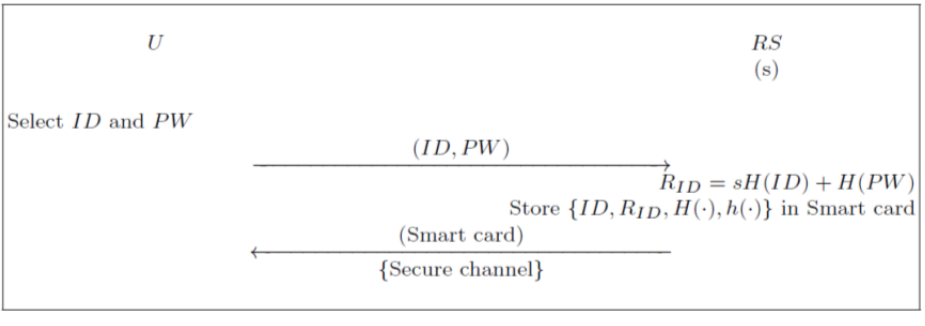

Fig. 1. Registration phase of GDS scheme

3.2 Login and verification phase

In this phase, the user U wants to communicate with the powerful server RS. This phase is depicted in Figure 2. The detailed communication steps are described as follows:

L1. $U \rightarrow RS: (ID, DID, V, T)$

(a) U inserts smart card in a terminal and submits ID and PW.

(b) After validating the ID, the smart card randomly chooses an integer $r \in Z_q^*$.

(c) The smart card computes $V(V_x, V_y) = rP_S$.

(d) The smart card computes $DID = (r + h(T, V_x, V_y))[R_{ID} - H(PW)]$, where T is the user system's timestamp.

(e) The smart card sends (ID, DID, V, T) to RS over a public channel.

L2. $RS \rightarrow U$: (Accept or Reject)

RS receives (ID, DID, V, T) at time T^* and verifies the validity of the time interval between T^* and T, by checking if $(T^* - T) \leq \Delta T$. If it holds, checks whether

$$e(DID, P) \stackrel{?}{=} e(H(ID), V + h(T, V_x, V_y)P_S) \quad (1)$$

If it holds, RS accepts the login request, rejects otherwise.

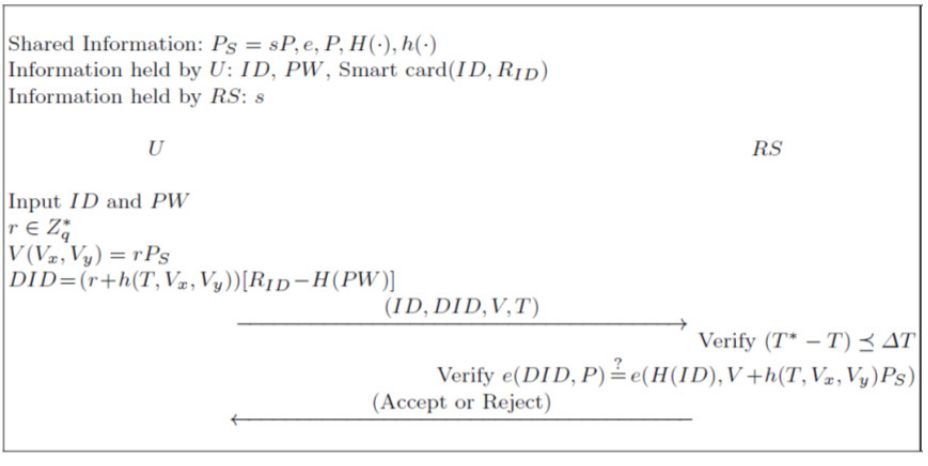

Fig. 2. Login and verification phase of GDS scheme

3.3 Password change phase

P1. U inserts the smart card into a terminal and submits ID and password PW.
P2. The smart card verifies the entered ID with the stored one in the smart card. If ID is matched, it prompts U for a new password PW^*.
P3. U submits a new password PW^*.
P4. The smart card computes

$$\begin{aligned} R_{ID}^* &= R_{ID} - H(PW) + H(PW^*) \\ &= sH(ID) + H(PW^*) \end{aligned} \quad (2)$$

and replaces the previously stored R_{ID} by R_{ID}^*.

4 Cryptanalysis of GDS scheme

This section shows that the GDS scheme is not only insecure against off-line password guessing, remote server impersonation, Denial of Service, and insider attacks, but also has mutual authentication problem.

4.1 Off-line password guessing attack

GDS scheme is vulnerable to the off-line password guessing attack as follows. Suppose that an adversary has obtained $(ID, R_{ID}, H(\cdot), h(\cdot))$ stored in the stolen smart card, the adversary can guess a candidate password PW_a^*, and then check whether

$$e(R_{ID} - H(PW_a^*), P) = e(H(ID), P_S) \quad (3)$$

If the check holds valid, which implies $PW = PW_a^*$, the adversary has success- fully guessed U's password. Otherwise, the adversary tries another candidate password. Thus, GDS scheme cannot resist the off-line password guessing attack.

4.2 Remote server impersonation attack

GDS scheme is vulnerable to the remote server impersonation attack. In GDS scheme, anyone can verify the validity of login request message (ID, DID, V, T) of U beside the remote server. That is, an adversary can easily authenticate the user U by performing the verification equation (1) with the login request message (ID, DID, V, T) and the remote server RS's public key $P_S = sP$. We can see that the verification equation (1) does not require the remote server RS's private key s. It means that an adversary can perform the following remote server impersonation attack. Suppose that an adversary has intercepted (ID, DID, V, T) in the login and verification phase and obtained the RS's public key $P_S = sP$, then he/she can easily check the validity of the timestamp T and whether $e(DID, P)$?= $e(H(ID), V + h(T, V_x, V_y)P_S)$. If both checks hold valid, the adversary accepts the login request, rejects otherwise. Thus, GDS scheme cannot resist the remote server impersonation attack.

4.3 DoS attack on password change phase

Suppose that an adversary temporarily gets U's smart card in the password change phase of the GDS scheme, then he/she can arbitrarily input two passwords PW_{old} and PW_{new} as the old and the new ones, respectively. In this case, the smart card will compute

$$R_{ID}^{*} = R_{ID} - H(PW_{old}) + H(PWnew)$$
$$= sH(ID) + H(PW) - H(PW_{old}) + H(PWnew)$$

and replace R_{ID} with R_{ID}^{*}. As a result, this will make U 's original password PW never be used in subsequent login and verification phase and thus cause denial of service.

4.4 Mutual authentication problem

GDS scheme does not provide secure mutual authentication. Mutual authentication means that both client and server are authenticated to each other within the same protocol. In Step L2 of the GDS scheme, RS can authenticate U by checking the equation (1) because only a valid U can compute DID of the equation (3). However, U cannot authenticate RS because RS does not send any authentication message to U for mutual authentication. It means that an attacker can easily impersonate a legal remote server to cheat the user U without performing the authentication procedure. Therefore, the GDS scheme cannot achieve mutual authentication.

4.5 Insider attack

GDS scheme is vulnerable to the insider attack. The insider attack means that the insider attacker of RS can directly obtain the user U 's password PW in the registration phase [23, 24]. In the GDS scheme, users' passwords PW will be directly revealed to RS because they are transmitted to RS as plaintext, so RS can get all the users' passwords PW in the registration phase. The insider attacker of RS can use these passwords to access other servers to provide useful services or information instead of U. In practice, users offer the same password to access several remote servers for their convenience. Thus the insider attacker of the remote server may try to use PW to impersonate U to login to the other remote servers that U has registered with outside this server. If the targeted outside remote server adopts the normal password authentication scheme, it is possible that the insider attacker of the remote server could successfully impersonate U to login to it by using PW. Although it is also possible that all the insiders of the remote server can be trusted and that U does not use the same password to access several servers, the implementers and the users of the scheme should be aware of such a potential weakness [12,13]. Therefore, GDS scheme is vulnerable to the insider attack.

5 Conclusions

This paper showed that the GDS scheme is not only insecure against off-line password guessing, server impersonation, DoS, and insider attacks, but also has

secure mutual authentication problem. Thus, the GDS scheme cannot be applicable to real client-server communication environments. Further works will be focused on improving the GDS scheme which can be able to provide greater security and provides computation efficiency.

Acknowledgments. We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This study was supported by the Kyungil University Grant.

References

1. L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol.24, no.11, pp.770-772, 1981.
2. C.C. Chang and W.Y. Liao, "A remote password authentication scheme based upon ElGamal's signature scheme," Computers & Security, vol.13, no.2, pp.137-144, 1994.
3. D.P. Jablon, "Strong password-only authenticated key exchange," ACM Computer Communications Review, vol.26, no.5, pp.5-20, 1996.
4. Y.Y. Wang, J.Y. Liu, F.X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Computer Communications, vol.32, no.4, pp.583-585, 2009.
5. S.K. Kim and M.G. Chung, "More secure remote user authentication scheme," Computer Communications, vol.32, no.6, pp.1018-1021, 2009.
6. J. Xu, W.T. Zhu, and D.G. Feng, "An improved smart card based password authentication scheme with provable security,", Computer Standards & Interfaces, vol.31, no.4, pp.723-728, 2009.
7. C.T. Li and M.S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol.33, no.1, pp.1-5, 2010.
8. A. Joux, "A one round protocol for tripartite Diffie-Hellman," in: Proceedings of Algorithmic Number Theory Symposium Lecture Notes in Computer Science, vol.1838, Springer-Verlag, Berlin, pp.385-394, 2000.
9. M.L. Das, A. Saxena, V.P. Gulati, and D.B. Phatak, "A novel remote user authentication scheme using bilinear pairings," Computers & Security, vol.25, no.3, pp.184-189, 2006.
10. J.S. Chou, Y. Chen, and J.Y. Lin, "Improvement of Das et al.'s remote user authentication scheme," Cryptology ePrint Archive, Report 2005/450, 2005.
11. T. Goriparthi, M. Das, and A. Saxena, "An improved bilinear pairing based remote user authentication scheme," Computer Standards & Interfaces, vol.31, no.1, pp.181-185, 2009.
12. W.C. Ku, H.M. Chuang, and M.J. Tsaur, "Vulnerabilities of Wu-Chieu's improved password authentication scheme using smart cards," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E88-A, no.11, pp.3241-3243, 2005.
13. E.J. Yoon and K.Y. Yoo, "Two security problems of efficient remote mutual authentication and key agreement," in: Proceedings of Future Generation Communication and Networking (FGCN 2007), vol.2, pp.66-70, 2007.